

Số: /SYT-TCHC  
V/v thông báo tình hình an toàn,  
an ninh mạng tháng 01/2026

Hải Phòng, ngày tháng năm 2026

Kính gửi:

- Các phòng, các đơn vị trực thuộc Sở;
  - Các cơ sở khám bệnh, chữa bệnh trên địa bàn thành phố.
- (Sau đây gọi là các đơn vị)

Ngày 03/02/2026, Sở Y tế nhận được Văn bản số 926/CAHP-ANM của Công an thành phố Hải Phòng về việc thông báo tình hình an toàn, an ninh mạng tháng 01/2026.

Căn cứ tình hình an ninh mạng tháng 01/2026 qua Thông báo của Phòng An ninh mạng - Công an thành phố Hải Phòng, Sở Y tế đề nghị Thủ trưởng các đơn vị thực hiện nghiêm các quy định về bảo đảm an toàn, an ninh mạng cho các hệ thống thông tin thuộc phạm vi quản lý, cụ thể:

a) Tổ chức các hoạt động tuyên truyền, nâng cao nhận thức kỹ năng cơ bản về an toàn thông tin mạng; Nhận biết, cảnh giác trước thông tin xấu độc, tin giả, thông tin xuyên tạc, chống phá, chính sách của Đảng và Nhà nước; Phòng, chống lừa đảo trên không gian mạng cho toàn thể cán bộ và người lao động của đơn vị quản lý.

b) Rà soát các hệ thống thông tin, bảo đảm các hệ thống thông tin được triển khai đầy đủ các biện pháp bảo vệ theo cấp độ an toàn. Chủ động rà soát, xử lý, triển khai các giải pháp nhằm khắc phục triệt để việc cập nhật, bảo mật đối với các trang website; cập nhật các phiên bản mới nhất của các trình duyệt web (Google Chrome, Cốc Cốc, Microsoft Edge, FireFox...) và các phiên bản mới nhất của Window nhằm khắc phục những lỗ hổng bảo mật của trình duyệt web

Chính phủ đã ban hành Nghị định quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân. Nghị định gồm 5 chương, 42 điều có hiệu lực kể từ ngày 01/01/2026, được ban hành nhằm cụ thể hóa phạm vi điều chỉnh, phân

loại dữ liệu, bảo đảm quyền của chủ thể dữ liệu, từ đó hoàn thiện khung pháp lý và tăng cường hiệu lực quản lý nhà nước trong môi trường số Việt Nam.

- Các chuyên gia đã phát hiện một loại mã độc, được đặt tên là MacSync, được phân phối thông qua một ứng dụng swift ký và chứng thực để vượt qua kiểm soát của Apple, nhằm mục đích tải xuống và thực thi mã độc trong DMG giả trình cài đặt hợp pháp, sau đó thực thi kịch bản được mã hóa và sử dụng các biện pháp né tránh như kiểm tra kết nối, giới hạn thời gian và bỏ thuộc tính cách ly, đồng thời chuyển dữ liệu và có thể điều khiển từ xa.

- Trong tháng 01/2026, tin tặc đã thực hiện chiến dịch tấn công mạng sau:

+ Chiến dịch mang tên PCPCat, là một chiến dịch gián điệp tự động hóa, nhắm vào Next.js và React, gây nhiễu loạn hạ tầng đám mây và thu thập dữ liệu quy mô lớn. Tin tặc khai thác các lỗ hổng để xâm nhập 59.128 máy chủ trong dưới 48 giờ và tỉ lệ tấn công thành công lên tới 64,6%. Hiện nay, chiến dịch này vẫn đang được thực hiện và dự kiến sẽ có thể tiếp tục xâm nhập hơn 1,2 triệu máy chủ, do đó, nhà phát hành khuyến nghị người dùng tạm thời chặn IP C2 (67.217.57.240) và thay đổi ngay các thông tin đăng nhập bị lộ trong các tệp môi trường.

+ Chiến dịch tấn công mang tên Zoom Stealer, sử dụng tiện ích mở rộng trên trình duyệt Chrome, Firefox và Edge, thu thập dữ liệu liên quan đến các cuộc họp trực tuyến như URL, ID, chủ đề, mô tả và mật khẩu nhúng, thông qua 18 tiện ích mở rộng. Các tiện ích này yêu cầu quyền truy cập vào 28 nền tảng hội họp, quyền tải xuống video, ghi âm và sau đó truyền dữ liệu được đánh cắp qua WebSocket tới tin tặc. Người dùng cần cảnh giác khi thấy tiện ích mở rộng yêu cầu cấp các quyền nhạy cảm trên.

+ Chiến dịch lừa đảo qua email lợi dụng tính năng gửi Email của Google Cloud Application Integration để phát tán thư giả mạo từ các tên miền thuộc Google, nhằm vượt qua cơ chế DMARC/SPF và nhắm vào hàng nghìn người dùng ở nhiều khu vực, bằng cách mô phỏng các thông báo doanh nghiệp và dẫn người dùng đến trang đăng nhập giả mạo của Microsoft. Người dùng cần cảnh giác, đánh giá kỹ càng

email gửi đến trước khi thực hiện các hành động tiếp theo. Các nhà nghiên cứu về bảo mật đã phát hiện một tiện ích mở rộng của Chrome mang tên Phantom Shuttle trên Chrome Web Store giả mạo là các công cụ proxy nhằm chiếm đoạt lưu lượng truy cập và đánh cắp dữ liệu nhạy cảm. Người dùng cần nâng cao cảnh giác và cài đặt các tiện ích mở rộng từ các nguồn tin cậy.

- Trong tháng 01/2026, các công ty an ninh mạng đã công bố các lỗ hổng bảo mật sau:

+ Lỗ hổng React2Shell (CVE-2025-55182) là một lỗ hổng giải mã dữ liệu không an toàn trong giao thức Flight của React Server Components (RSC) được sử dụng bởi thư viện React và framework Next.js. Lỗ hổng này có thể bị khai thác từ xa mà không cần xác thực để thực thi mã JavaScript trên máy chủ và hiện đang bị khai thác trong thực tế.

+ Lỗ hổng CVE-2026-0625 cho phép thực thi lệnh từ xa trên các bộ định tuyến DSL D-Link cũ. Vấn đề bắt nguồn từ việc vô hiệu hóa không đúng cách các thành phần đặc biệt dùng trong Lệnh hệ điều hành và chèn lệnh qua dnscfg.cgi. Tin tặc có thể chèn và thực thi shell tùy ý mà không cần xác thực. Các mẫu bị khai thác cụ thể là DSL-2740R, DSL-2640B...

+ Microsoft đã phát hành bản vá bảo mật quy mô lớn, khắc phục tổng cộng 114 lỗ hổng trên nhiều thành phần cốt lõi của hệ sinh thái Windows và Microsoft 365. Trong đó, có 08 lỗ hổng nghiêm trọng và 106 lỗ hổng ở mức quan trọng, trải dài từ Windows NTFS, Desktop Window Manager cho tới các driver cập nhật trong nhân hệ điều hành. Có 03 lỗ hổng Zero-day được vá, trong đó có 01 lỗ hổng đã được khai thác trong thực tế. Đây là bản vá cần được ưu tiên hàng đầu đối với các đội ngũ an ninh và quản trị hệ thống. Trong tháng 01/2026, Hệ thống quản lý mã độc tập trung của thành phố đã phát hiện 773 thiết bị thuộc 82 tổ chức trên địa bàn thành phố Hải Phòng có tình trạng mất an ninh mạng, với tổng cộng 1614 mối đe dọa từ mã độc, link giả mạo, 14607 file độc hại. Qua công tác quản lý và nắm tình hình, Công an thành phố đã phát hiện tình trạng mất an ninh mạng, an toàn thông tin đối với Hệ thống thông tin Công ty cổ phần Cảng Hải Phòng và Hệ thống thông tin Thành đoàn

Hải Phòng; Công an thành phố đã thông báo và phối hợp với các đơn vị trên để làm rõ, kịp thời khắc phục.

Sở Y tế yêu cầu Thủ trưởng các đơn vị chỉ đạo thực hiện, chủ động cập nhật và nâng cấp giải pháp về bảo đảm an toàn, an ninh mạng đối với hệ thống thông tin./.

***Nơi nhận:***

- Như trên;
- Công an TP (để p/h);
- Giám đốc và PGĐ SYT;
- Các phòng thuộc Sở;
- Lưu: VT, TCHC (ĐVH).

**KT. GIÁM ĐỐC  
PHÓ GIÁM ĐỐC**

**Phan Huy Thục**